



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.				
09/944,694	08/31/2001	Matthew Gast	NC30561	2124				
<div>7590 Brian T. Rivers, Esq. Nokia, Inc. Mail drop 1-4-755 6000 Connection Dr. Irving, TX 75039</div>								
<div>02/05/2008</div>								
<div>EXAMINER. HA, LEYNNA A</div>								
<table border="1"><thead><tr><th>ART UNIT</th><th>PAPER NUMBER</th></tr></thead><tbody><tr><td>2135</td><td></td></tr></tbody></table>					ART UNIT	PAPER NUMBER	2135	
ART UNIT	PAPER NUMBER							
2135								
<table border="1"><thead><tr><th>MAIL DATE</th><th>DELIVERY MODE</th></tr></thead><tbody><tr><td>02/05/2008</td><td>PAPER</td></tr></tbody></table>					MAIL DATE	DELIVERY MODE	02/05/2008	PAPER
MAIL DATE	DELIVERY MODE							
02/05/2008	PAPER							

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

**Application No.**

09/944,694

**Applicant(s)**

GAST, MATTHEW

**Examiner**

LEYNNA T. HA

**Art Unit**

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 19 November 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-12 and 14-18 is/are pending in the application.
- 4a) Of the above claim(s) 13 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-12 and 14-18 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Claims 1-12 and 14-18 are pending.

Applicant have cancelled claim 13.

#### ***Response to Arguments***

2. ***Applicant's arguments with respect to claims 3 and 12-18 have been considered but are moot in view of the new ground(s) of rejection.***

3. ***Applicant's arguments filed 11/29/2007 have been fully considered but they are not persuasive.***

Claims 1, 2, and 4-11 remains rejected over the Grabelsky and Zarom combination.

Regarding the argument on pg.7, where Grabelsky does not teach or suggest translating a first plurality of cleartext data into a second plurality of cleartext data. Although Grabelsky teaches the header-field includes a type of data contained in the payload data-field (col.23, lines 11-17), but did not clearly point out this the translation of the cleartext data into another form. Thus, Zarom is brought forth to teach this limitation.

The argument pg.8 (2<sup>nd</sup> paragraph), regarding Grabelsky's router does not modify contents of received, secured (IPSEC) packets since to do so would compromise the security of those packets and cited some columns (i.e. col.3-4 and

Art Unit: 2135

col.25). However, applicant points to passages that are either explaining the background of the invention which usually consists of history of prior art relating to Grabelsky's invention or the disadvantages that are known problems with the methods or techniques of other or previous inventions. Then points out the advantages or the method to solve (overcome) the known problems with his method and technique of his invention (col.4, line 24-col.5, line 28 and col.49-52). Which according to Grabelsky's invention is to overcome some of the problems of violating the IPSec using NAT routers that are known to modify packets by allowing IPSec to be used with distributed network address translation (see abstract). Grabelsky points out there are "known" problems associated with using current versions of network address translation when security is required and the Internet Protocol security protocol is used, which suggests known disadvantages of this technique in the prior art (col.3, lines 55-67). Thus, Grabelsky indicated that it is desirable to allow network address translation when Internet Protocol security is being used to protocol Internet Protocol packets (col.4, lines 24-30). Further, Grabelsky discloses the router issues security certificates and may itself be authenticated by a higher certificate authority (col.5, lines 10-27). Rather than using NAT devices, DNAT can be used with IPSec to overcome the problems with NAT devices known in the art (col.25, lines 49-61). Thus, Grabelsky does not teach the insecure use or method of routers, rather provides protection and security for IP packets (as claimed) by using IPSec to establish secure connection to network devices (col.21, lines 4-50 and col.25, lines 53-col.26, line 25). Therefore, Grabelsky reads on the claimed method of providing network security of claim 1 and 2.

Art Unit: 2135

As for Zarom, is combined with Grabelsky to translate cleartext data. The claimed invention does not suggest nor can it be interpreted as modifying data because translating can broadly be given as interpreting or correspond to another form or type. For instance, address translation is known in the art as address A corresponds to address B that masks the real address so as to protect the real address from being exposed. Another example is described by the Zarom reference. Zarom teaches various examples of cleartext data into another cleartext data or (language) format translated to another format (col.3, lines 26-37): HTML to WML (col.1, lines 57-58), TCP packets to WTP packets (col.7, lines 58-60), WAP to TCP packets (col.9, lines 40-50), IP packet to a WAP network packet (col.6, lines 55-58). Zarom teaches it would have been obvious for a person of ordinary skills in the art to combine the teaching of Grabelsky with the teaching of translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule as taught by Zarom because the increasing demand for different types of communication services through the increasing popular portable electronic devices (col.1, lines 14-22) that there is a need to extend the power and efficacy of operation of portable, wireless electronic communication devices. Thus, Zarom teaches translating at IP level is faster and efficient in order to effectively to communicate deliver content from the Internet (col.1, lines 50-63 and col.6, lines 21-35).

As for dependent claims, they are also rejected by virtue of dependency.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

**4. Claims 1, 2, and 4-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grabelsky, et al. (US 7,032,242) in view of Zarom (US 6,356,529).**

**As per claim 1:**

Grabelsky, et al. discloses a method for providing network security, comprising the steps of:

receiving a plurality of network protocol packets, wherein a network protocol packet includes a network protocol header (**col.20, lines 49-50**) and a plurality of network protocol data, and wherein the network protocol data include a first cryptographic protocol header (**col.21, lines 17-21**) and a first plurality of encrypted data, at least a portion of at least some of the network protocol packets being configured in accordance with a transport layer protocol or a network layer protocol; (**col.11, lines 55-56**)

determining a first plurality of cryptographic protocol rules associated with the network protocol data; (**col.21, lines 4-13 and col.22, lines 63-55**)

establishing a cryptographic session, if required by said first cryptographic rules;

**(col.24, lines 34-40)**

applying the first plurality of cryptographic protocol rules to the first encrypted data to obtain a first plurality of cleartext data; **(col.23, lines 49-62; the claimed applying a cryptographic protocol rules to the encrypted data is logically to decrypt the received encrypted data in order to obtain the cleartext data as claimed. Grabelsky discloses for inbound packets at the receiving endpoint where the IP packet includes an ESP header and determines the appropriate SA. The SA indicates what encryption techniques should be used for the decryption whereby decryption involves using a key, decryption technique, and cryptographic synchronization data if any, is indicated by the SA (col.23, lines 55-61). The first plurality of cleartext data can broadly be given as decryption of the inbound data. Thus, Grabelsky reads on the claimed invention.)**

*[translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule]*

encrypting the second plurality of cleartext data in accordance with at least one rule associated with a second cryptographic protocol, resulting in a second plurality of encrypted data. **(col.23, lines 27-32; The second plurality of cleartext data can broadly be given as outbound data, where sending data to another endpoint obviously needs protection. Hence, Grabelsky discloses the sending endpoint encapsulates into the ESP payload data-field and original upper layer protocol information for the transport mode using the selected encryption technique.**

**Grabelsky reads on the encrypting with the rule associated with a cryptographic protocol.)**

However, Grabelsky did not provide translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule.

Zarom discloses a method and system for translating data transmitted according to the WAP network protocols in the lower protocol layers rather than requiring the packet to be transformed into higher layers (col.4, lines 52-64). Zarom discloses there is an increasing demand for different types of communication services through the increasing popular portable electronic devices (col.1, lines 14-22) that there is a need to extend the power and efficacy of operation of portable, wireless electronic communication devices. WAP (wireless application protocol) has been developed and designed to efficiently provide both multimedia and telephony services to wireless communication devices (col.1, lines 24-33) and provides the required adaptations and modifications to such software and data transmission protocols. Such adaptations and modifications includes a translation system or gateway to translate HTML to form WML (col.1, lines 54-62). Zarom further suggests that current available translators in the art require the data to be translated only at the highest (application) level of the network protocols and involves two separate sessions are operated with significant delays in each session for the translation process (col.6, lines 28-32), where the proxy server waits for the translation process to be completed for each of original server and wireless communication device client before the translated data can be passed to the other session (col.2, lines 20-34 and col.3, lines 15-17). Thus, this method significantly



Art Unit: 2135

decreases the efficiency of these background art translators and their translation process (col.2, lines 37-39 and col.6, lines 28-32). However, Zarom' solution would be able to pass translated information as soon as only a portion is translated according to rules (col.3, lines 8-15 and col.7, lines 12-30) and the translation process is performed entirely at the IP level rather than at the application level (col.6, lines 21-28). Zarom teaches data must be converted through all of the network layers before translation and must be reconverted to a format which is suitable for transmission through the physical network media (col.2, lines 23-28). Thus, is more efficient which is able to translate packets more rapidly from protocol type to the other than background art translators (col.2, lines 40-54 and col.6, lines 32-34). Zarom discloses the translator receiving either regular IP packets and WAP packets or other wireless network packets (col.7, lines 32-34). Zarom shows the examples of cleartext data into another cleartext data or (language) format translated to another format (col.3, lines 26-37): HTML to WML (col.1, lines 57-58), TCP packets to WTP packets (col.7, lines 58-60), WAP to TCP packets (col.9, lines 40-50), IP packet to a WAP network packet (col.6, lines 55-58).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Grabelsky with the teaching of translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule as taught by Zarom because translating at IP level is faster and efficient in order to effectively to communicate deliver content from the Internet (col.1, lines 50-63 and col.6, lines 21-35).

**As per claim 2:**

Art Unit: 2135

Grabelsky discloses a system for providing network security, comprising:

an input module for receiving a plurality of network protocol packets (**col.20, lines 49-50**), at least a portion of at least some of the network protocol packets being configured in accordance with a transport protocol or a network layer protocol; (**col.11, lines 55-56 and col.21, lines 17-21**)

*(a translation module for translating a first plurality of data into a second plurality of data)*

an output module; and (**col.23, lines 21-22**)

a cryptographic module responsive to the input module and the output module for performing cryptographic operations. (**col.23, lines 21-62**)

However, Grabelsky did not provide a translation module for translating a first plurality of data into a second plurality of data.

Zarom discloses a method and system for translating data transmitted according to the WAP network protocols in the lower protocol layers rather than requiring the packet to be transformed into higher layers (col.4, lines 52-64). Zarom discloses there is an increasing demand for different types of communication services through the increasing popular portable electronic devices (col.1, lines 14-22) that there is a need to extend the power and efficacy of operation of portable, wireless electronic communication devices. WAP (wireless application protocol) has been developed and designed to efficiently provide both multimedia and telephony services to wireless communication devices (col.1, lines 24-33) and provides the required adaptations and modifications to such software and data transmission protocols. Such adaptations and

Art Unit: 2135

modifications includes a translation system or gateway to translate HTML to form WML (col.1, lines 54-62). Zarom further suggests that current available translators in the art require the data to be translated only at the highest (application) level of the network protocols and involves two separate sessions are operated with significant delays in each session for the translation process (col.6, lines 28-32), where the proxy server waits for the translation process to be completed for each of original server and wireless communication device client before the translated data can be passed to the other session (col.2, lines 20-34 and col.3, lines 15-17). Thus, this method significantly decreases the efficiency of these background art translators and their translation process (col.2, lines 37-39 and col.6, lines 28-32). However, Zarom's solution would be able to pass translated information as soon as only a portion is translated according to rules (col.3, lines 8-15 and col.7, lines 12-30) and the translation process is performed entirely at the IP level rather than at the application level (col.6, lines 21-28). Zarom teaches data must be converted through all of the network layers before translation and must be reconverted to a format which is suitable for transmission through the physical network media (col.2, lines 23-28). Thus, is more efficient which is able to translate packets more rapidly from protocol type to the other than background art translators (col.2, lines 40-54 and col.6, lines 32-34). Zarom discloses the translator receiving either regular IP packets and WAP packets or other wireless network packets (col.7, lines 32-34). Zarom shows the examples of cleartext data into another cleartext data or (language) format translated to another format (col.3, lines 26-37): HTML to WML (col.1,

Art Unit: 2135

lines 57-58), TCP packets to WTP packets (col.7, lines 58-60), WAP to TCP packets (col.9, lines 40-50), IP packet to a WAP network packet (col.6, lines 55-58).

Therefore, it would have been obvious for a person of ordinary skills in the art at the time of the invention was made to combine the teaching of Grabelsky with the teaching of translating the first plurality of cleartext data into a second plurality of cleartext data in accordance with at least one translation rule as taught by Zarom because translating at IP level is faster and efficient in order to effectively to communicate deliver content from the Internet (col.1, lines 50-63 and col.6, lines 21-35).

**As per claim 4:** See Zarom on col.3, lines 8-15 and col.7, lines 12-30; discussing at least one translation rule is predetermined.

**As per claim 5:** See Zarom on col.7, lines 12-30 and 55-67; discussing at least one translation rule is determined dynamically.

**As per claim 6:** See Grabelsky on col.7, lines 10-12 and Zarom on col.3, lines 5-6; discussing the first cryptographic protocol is WTLS.

**As per claim 7:** See Zarom on col.5, lines 37-46; discussing the first plurality of encrypted data is associated with WML.

**As per claim 8:** See Grabelsky on col.7, lines 10-12 and Zarom on col.3, lines 57-58; discussing second plurality of encrypted data is associated with HTML.

**As per claim 9:** See Zarom on col.8, lines 7-11; discussing the second cryptographic protocol is SSL over HTTP.

**As per claim 10:** See Grabelsky on col.22, lines 62-65 and col.23, lines 50-62; discussing the first cryptographic protocol and the second cryptographic protocol are

Art Unit: 2135

identical.

**As per claim 11: See Grabelsky on col.22, lines 62-65 and col.23, lines 50-62;**  
discussing the first plurality of encrypted data and the second plurality of encrypted data  
conform to different revisions of a specification for the same cryptographic protocol.

**5. Claims 3 and 12-18 are rejected under 35 U.S.C. 103(a) as being  
unpatentable over of Chang, et al. (US 6,963,972) in view Barlow, et al. (US  
6,810,479)**

**As per claim 3:**

Chang, et al. discloses a system for providing network security, comprising:

means for receiving a request to perform a cryptographic operation; (*col.6, lines  
65-67 and col.7, lines 8-12*)

means for returning a response to the cryptographic operation request; (*col.6,  
lines 40-45 and col.11, lines 55-63*)

means for translating a first plurality of cleartext data into a second plurality of  
cleartext data in accordance with at least one translation rule; and (*col.4, lines 13-19  
and col.6, lines 30-33; Chang discloses transcoding refers to the technique of  
transforming multimedia content from a first original format into a second format (col.1,  
lines 16-20). The terms translation, content repurposing, content adaptation,  
reformatting, data transformation, media conversion, format conversion, and filtering are  
often used synonymously for transcoding (col.2, lines 23-27). The claimed translating a*

Art Unit: 2135

***first cleartext data into a second plurality of cleartext data is where Chang transcode or convert an original format into a second format.)***

at least one module for performing said cryptographic operations, said cryptographic operations including obtaining the first plurality of cleartext data based upon a first plurality of encrypted data (***col.4, lines 9 and 20-22 and col.10, lines 52-62***), and encrypting the second plurality of cleartext data to obtain a second plurality of encrypted data (***col.7, lines 50-58 and col.10, lines 1-12***), cryptographic operations are performed using *[cryptographic acceleration hardware]*.

Barlow is combined with Chang to better explain the cryptographic acceleration hardware. Barlow discloses the cryptographic acceleration circuitry is integrated with the CPU which streamlines cryptography computations to improve speed. The cryptography accelerator performs certain cryptographic functions including encryption, decryption, signing and verification (***col.11, lines 50-62***). Therefore, it would have been obvious for a person of ordinary skills in the art to combine Chang with Barlow to teach an cryptographic acceleration hardware because it performs certain cryptographic functions including encryption, decryption, signing and verification that streamlines cryptography computations to improve speed (***Barlow-col.11, lines 50-62***).

As per claim 12: See Chang col.7, lines 34-35; discussing at least one cryptographic module is a cryptographically strong pseudorandom number generator.

As per claim 14: See Chang col.6, lines 40-67 and Barlow-col.11, lines 50-62; discussing the cryptographic acceleration hardware includes a plurality of individual hardware acceleration units.

Art Unit: 2135

As per claim 15: See Chang col.6, lines 65-67 and Barlow-col.11, lines 50-62; discussing at least one individual hardware acceleration unit is dedicated to one function.

As per claim 16: See Chang col.3, lines 21-28 and Barlow-col.11, lines 50-62; discussing the cryptographic acceleration hardware is updateable by loading at least one cryptographically signed instruction.

As per claim 17: See Chang col.9, lines 59-67 and Barlow-col.11, lines 50-62; discussing the cryptographic acceleration hardware is tamper-resistant.

As per claim 18: See Chang col.9, lines 59-67 and Barlow-col.11, lines 50-62; discussing the cryptographic acceleration hardware is tamper-evident.

### ***Conclusion***

**6. THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In

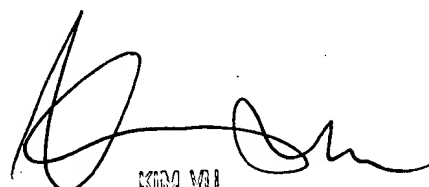
no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

LHa



KIM VU  
USPTO PATENT EXAMINER  
FACSIMILE